

BUILDING EXTREMAL FEWNOMIAL LOWER BOUNDS OVER LOCAL FIELDS, AND THE ADELIC TAU CONJECTURE

J. MAURICE ROJAS

To Bernd Sturmfels on his 50th birthday.

ABSTRACT. Consider a system F of n polynomials in n variables, with a total of $n + k$ distinct exponent vectors, over any local field L . We discuss conjecturally tight upper and lower bounds on the maximal number of non-degenerate roots F can have over L , with all coordinates having fixed sign or fixed first digit, as a function of n and k only. For non-Archimedean L we give the first non-trivial lower bounds in the case $k - 1 \leq n$; and for general L we give new explicit extremal systems when $k = 2$ and $n \geq 1$. We also briefly review the background behind such bounds, and their application, including connections to variants of the Shub-Smale τ -Conjecture and the **P** vs. **NP** Problem. One of our key tools is the construction of combinatorially constrained tropical varieties with maximally many intersections.

1. MAIN RESULT AND NEW CONJECTURES

Let L be any local field, i.e., \mathbb{C} , \mathbb{R} , or any finite algebraic extension of \mathbb{Q}_p or $\mathbb{F}_p((t))$ [Ser79]. Also let $f_1, \dots, f_n \in L[x_1^{\pm 1}, \dots, x_n^{\pm 1}]$ be Laurent polynomials such that the total number of distinct exponents in the monomial term expansions of f_1, \dots, f_n is $n + k$. We call such an $F = (f_1, \dots, f_n)$ an $n \times n$ $(n + k)$ -*nomial system over L* . We will study the maximal number of non-degenerate roots of F , in the multiplicative group $(L^*)^n$, as a function of n and k only. This is the basic quantitative problem of *fewnomial theory over local fields*.

That such bounds could actually be finite was first observed by Descartes around 1637 for $(L, n) = (\mathbb{R}, 1)$ [SL54]. About three and a half centuries later, Khovanskii and Sevastyanov extended this result to $n \geq 2$ (still with $L = \mathbb{R}$) [Kho80, Kho91], and then Denef, van den Dries, Lenstra, Poonen, and Rojas showed that the same could be done for more general L [DvdD88, Poo98, Len99, Roj04]. Fewnomial theory over \mathbb{R} has since found applications in Hilbert's 16th Problem [Kal03], algorithmic complexity [GV01, VG03, BRS09, PRT09, BS09, Koi10], model completeness for certain theories of real analytic functions [Wil99], and the study of torsion points on curves [CZ02]. Fewnomial bounds over number fields have applications to sharper uniform bounds on the number of torsion points on elliptic curves [Che04], and additive complexity [Roj02]. Since any number field embeds in some finite extension of \mathbb{Q}_p , we thus have good reason to study fewnomial bounds over general local fields. However, for $n \geq 2$, or general local L , *tight* bounds remain elusive [LRW03, Roj04, BS07, AI10, AI11].

We will occasionally refer to the special case $L \in \{\mathbb{R}, \mathbb{C}\}$ as the *Archimedean* case. To simplify and broaden our perspective, let us introduce the following quantities.

Definition 1.1. Let $x \in L$. When $L \in \{\mathbb{R}, \mathbb{C}\}$ we let $|x|$ denote the usual absolute value and define the Archimedean valuation of x to be $\text{ord } x := -\log |x|$. We call $\phi(x) := \frac{x}{|x|}$ the generalized phase of x . In the non-Archimedean case, we let \mathfrak{M} denote the unique maximal ideal of the ring of integers of L and call any generator ρ of \mathfrak{M} a uniformizing parameter

Key words and phrases. sparse polynomial, tau conjecture, local field, positive characteristic, lower bounds, mixed cell, straight-line program, complexity.

Department of Mathematics, Texas A&M University TAMU 3368, College Station, Texas 77843-3368, USA. rojas@math.tamu.edu. Partially supported by NSF MCS grant DMS-0915245, DOE ASCR grant de-sc0002505, and Sandia National Laboratories.

for L . Letting ord denote the corresponding valuation on L we then alternatively define the generalized phase as $\phi(x) := \frac{x}{\rho^{\text{ord } x}} \bmod \mathfrak{M}$. Finally, for arbitrary local L , we define $\Omega_L(n, k)$ to be the maximal number of non-degenerate roots in L^n , with all coordinates having generalized phase 1, for any $n \times n$ $(n + k)$ -nomial system F over L . \diamond

Note that an $x \in \mathbb{R}$ (resp. $x \in \mathbb{Q}_p$) has generalized phase 1 iff x is positive (resp. has p -adic first digit 1). So Descartes' classic 17th century bound on the number of positive roots of a sparse univariate polynomial [SL54, Kho91, LRW03, Wan04], when combined with the simple extremal example $(x_1 - 1)(x_1 - 2) \cdots (x_1 - k)$, can be rephrased as the equality $\Omega_{\mathbb{R}}(1, k) = k$. Let \mathbb{R}_+ denote the positive real numbers.

Example 1.2. *The right-hand 4×4 polynomial system consists of trinomials but forms a 6-nomial system.*

(Those uncomfortable with this terminology can replace the 4 polynomials of G by generic linear combinations thereof, so that the resulting system has the same roots but then consists of 6-nomials.)

Applying the identity $x_1^2(x_2x_3)^2x_4^2 - (x_1x_2)^2(x_3x_4)^2 = 0$, it is then easily checked that, for any root $(\zeta_1, \zeta_2, \zeta_3, \zeta_4) \in (\mathbb{R}^)^4$ of G , the quantity $u := \zeta_1^2$ must satisfy $u(1 + \frac{1}{4}u)^2(1 + \frac{1}{4^5}u)^2 - (\frac{1}{4} + u)^2(1 + \frac{1}{4^3}u)^2 = 0$. Successively solving for $\zeta_4, \zeta_3, \zeta_2, \zeta_1$ via the fourth, third, second, and first equations then implies that G has no more than 5 roots in \mathbb{C}^4 , and a quick check via **Maple** reveals that this G has exactly 5 roots in \mathbb{R}_+^4 . This is the first explicit example to evince $\Omega_{\mathbb{R}}(4, 2) \geq 5$. \diamond*

$$G := \begin{cases} x_1x_2 - \frac{1}{4} - x_1^2 \\ x_2x_3 - 1 - x_1^2/4 \\ x_3x_4 - 1 - x_1^2/4^3 \\ x_4 - 1 - x_1^2/4^5 \end{cases}$$

For any field L (local or not) and $n \geq 1$, it is a simple linear algebra/unit group exercise to prove $\Omega_L(n, 1) = 1$ and $\Omega_L(n, k) = 0$ for all $k \leq 0$. However, until the present paper, the only non-trivial upper or lower bound known for $\Omega_{\mathbb{Q}_p}(n, 2)$ was an upper bound no greater than $3^n \lfloor (8.001n)^n \rfloor$ [Roj04]. So we give new lower bounds for $\Omega_L(n, k)$ in the non-Archimedean case, using *explicit* polynomial systems that evince such bounds over any local field L .

Theorem 1.1. *For $n, k \geq 1$ and any local field L we have $\Omega_L(n, k) \geq \left\lfloor \frac{n+k-1}{\min\{n, k-1\}} \right\rfloor^{\min\{n, k-1\}}$.*

The real lower bound $\Omega_{\mathbb{R}}(n, 2) \geq n + 1$ was first proved via a clever use of Dessins d'Enfants [Bih07] and then used to show that $\Omega_{\mathbb{R}}(n, k) \geq \left\lfloor \frac{n+k-1}{k-1} \right\rfloor^{k-1}$ for $1 \leq k - 1 \leq n$ in [BRS07]. Our more general lower bound also depends on the subcase $k = 2$, but here we attain the latter — for *all* $L \in \{\mathbb{R}\} \cup \{\mathbb{Q}_2, \mathbb{Q}_3, \mathbb{Q}_5, \dots\} \cup \{\mathbb{F}_2((t)), \mathbb{F}_3((t)), \mathbb{F}_5((t)), \dots\}$ — via an explicit family of polynomial systems. Letting \bar{L} denote the algebraic closure of L , our new family of extremal systems can be described as follows.

Theorem 1.2. *For any $n \geq 2$, any local field L , and any $q \in L^*$ with generalized phase 1 and ord q sufficiently large, the $n \times n$ $(n + 2)$ -nomial system*

$$G_\varepsilon := \begin{cases} x_1x_2 - (\varepsilon + x_1^2) \\ x_2x_3 - (1 + \varepsilon x_1^2) \\ x_3x_4 - (1 + \varepsilon^3 x_1^2) \\ \vdots \\ x_{n-1}x_n - (1 + \varepsilon^{2n-5} x_1^2) \\ x_n - (1 + \varepsilon^{2n-3} x_1^2) \end{cases}$$

has exactly $n + 1$ roots $(\zeta_1, \dots, \zeta_n)$ in \bar{L}^n , and all these roots lie in $(L^)^n$ and satisfy $\phi(\zeta_1) = \dots = \phi(\zeta_n) = 1$. In particular, when $L = \mathbb{Q}_p$ (resp. $L = \mathbb{F}_p((t))$, $L \in \{\mathbb{R}, \mathbb{C}\}$),*

$\varepsilon = p$ (resp. $\varepsilon = t$, $\varepsilon = 1/4$) implies G_ε has the aforementioned behavior for all $n \geq 2$ (resp. $n \geq 2$, $n \in \{2, \dots, 100\}$).

Explicit examples evincing $\Omega_{\mathbb{R}}(n, 2) \geq n + 1$ were previously known only for $n \leq 3$ [BRS07]. Our new extremal examples from Theorem 1.2 thus also provide a new (and arguably simpler) proof that $\Omega_{\mathbb{R}}(n, 2) \geq n + 1$. We prove Theorems 1.1 and 1.2 respectively in Sections 3.1 and 3.2.

Remark 1.3. *By construction, whether we are over \mathbb{Q}_p or $\mathbb{F}_p((t))$, the underlying tropical varieties of the zero sets defined by G_ε have a common form: they are each the Minkowski sum of an $(n - 2)$ -plane and a “Y” lying in a complementary 2-plane. Furthermore, all these tropical varieties contain half-planes parallel to a single $(n - 1)$ -plane. It is an amusing exercise to build such a collection of tropical varieties so that they have at least $n + 1$ isolated intersections. However, it is much more difficult to build a collection of polynomials whose tropical varieties have this property, and this constitutes a key subtlety behind Theorem 1.2. \diamond*

1.1. Upper Bounds: Known and Conjectural. Let us begin with results in one variable: Considerably refining earlier seminal work of Lenstra [Len99], Avendaño and Krick have recently obtained the bounds $2k - 1 \leq \Omega_{\mathbb{Q}_p}(1, k) \leq k^2 - k + 1$ for any prime p [AK10]. (Their results also yield similar upper bounds for any finite algebraic extension of \mathbb{Q}_p .) For L of positive characteristic, Poonen has proved tight upper bounds for the number of roots of a univariate $(k + 1)$ -nomial over L [Poo98]. A simple consequence of his development is the following explicit formula:

Proposition 1.4. $\Omega_{\mathbb{F}_q((t))}(1, k) = \frac{q^k - 1}{q - 1}$ for all $k \geq 1$ and any prime power q . ■

Indeed, separating the roots of generalized phase 1 by valuation, one sees from [Poo98, Sec. 2] that $\Omega_{\mathbb{F}_q((t))}(1, k) \leq 1 + q + \dots + q^{k-1}$. For the lower bound, the first example from [Poo98]

$$r_k(x_1) := \prod_{z_1, \dots, z_{k-1} \in \mathbb{F}_p} (x_1 - z_1 - z_2 t - \dots - z_{k-1} t^{k-1})$$

turns out to be a $(k + 1)$ -nomial in x_1 having exactly $1 + q + \dots + q^{k-1}$ roots of generalized phase 1 in $\mathbb{F}_p[t]$, each of which is non-degenerate.

More generally, the best general upper and lower bounds on $\Omega_L(n, k)$, for $L \in \{\mathbb{R}, \mathbb{Q}_2, \mathbb{Q}_3, \mathbb{Q}_5, \dots\}$ and $n, k \geq 2$ (as of December 2011) are:

	Upper Bound on $\Omega_L(n, k)$	Lower Bound on $\Omega_L(n, k)$
$L = \mathbb{R}$	$2^{O(k^2)} n^{k-1}$ [BS07] ¹	$\left\lfloor \frac{n+k-1}{\min\{n, k-1\}} \right\rfloor^{\min\{n, k-1\}}$ [LRW03, BRS07]
$L = \mathbb{Q}_p$	$(O(k^3 n \log k))^n$ [Roj04]	$\left\lfloor \frac{n+k-1}{\min\{n, k-1\}} \right\rfloor^{\min\{n, k-1\}}$ (Theorem 1.1 here)

Upper bounds on $\Omega_L(n, k)$ are still unknown for L of positive characteristic when $n \geq 2$ [Poo98]. As for lower bounds in positive characteristic, combining Proposition 1.4 with the polynomial system $(r_m(x_1), \dots, r_m(x_n))$ for $m = \lfloor \frac{n+k-1}{n} \rfloor$ immediately yields the following lower bound:

Proposition 1.5. $\Omega_{\mathbb{F}_q((t))}(n, k) \geq \left(\frac{q^{\lfloor \frac{n+k-1}{n} \rfloor} - 1}{q - 1} \right)^n > q^{k-n}$ for $1 \leq n \leq k - 1$ and any prime power q . ■

¹ While there have been important recent refinements to this bound (e.g., [RSS10]) the asymptotics of [BS07] have not yet been improved in complete generality.

No lower bounds for $\Omega_L(n, k)$ exponential in n appear to be known for the positive characteristic case when $n > k - 1$.

Most importantly, note that for the Archimedean case (resp. the characteristic 0 non-Archimedean case), $\Omega_L(n, k)$ is bounded above by a polynomial in n when k is fixed (resp. a polynomial in k when n is fixed). Based on this asymmetry of upper bounds, the author posed the following conjecture (mildly paraphrased) at his March 20 Geometry Seminar talk at the Courant Institute in March 2007.

The Local Fewnomial Conjecture.

There are absolute constants $C_2 > C_1 > 0$ such that, for any local field L of characteristic 0, and any $n, k \geq 2$, we have $(n + k - 1)^{C_1 \min\{n, k-1\}} \leq \Omega_L(n, k) \leq (n + k - 1)^{C_2 \min\{n, k-1\}}$.

Theorem 1.1 thus reveals the lower bound of the Local Fewnomial Conjecture to be true (with $C_1 = 1$) for the special case $k = 2$. From our table above we also see that the upper bound from the Local Fewnomial Conjecture holds for $n \leq k - 1$ (at least for $C_2 \geq 6$), in the characteristic 0 non-Archimedean setting. We intend for our techniques here to be a first step toward establishing the Local Fewnomial Conjecture for $n > k - 1$ in the characteristic 0 non-Archimedean setting.

Remark 1.6. *While the maximal number of roots in $(\mathbb{C}^*)^n$ of an $n \times n$ $(n+k)$ -nomial system F over \mathbb{C} is an unbounded function of n and k , it is in fact the case that $\Omega_{\mathbb{C}}(n, k)$ admits a $2^{O((n+k)^2)} n^{O(n+k)}$ upper bound. This is because Khovanski's Theorem on Complex Fewnomials gives finite (and explicit) lower and upper bounds on the number of roots F in any angular sector (see [Kho91, Cor. 8 & 9, pp. 80-81], [Kho91, Thm. 2, pp. 87-88], and the proofs in between). As the angular measure tends to zero, the resulting upper bound approaches a quantity close to $\Omega_{\mathbb{R}}(n, k)$. One may speculate that $\Omega_{\mathbb{C}}(n, k) = \Omega_{\mathbb{R}}(n, k)$ but the prescence of complex coefficients for F makes this less than obvious. \diamond*

Remark 1.7. *Should the Local Fewnomial Conjecture be true, it is likely that similar bounds can be asserted for the number of roots counting multiplicity. In fact, this is already known for $(L, n) = (\mathbb{R}, 1)$ [Wan04]. Also, the bounds from [Roj04] that gave evidence for the upper bounds in the characteristic 0 non-Archimedean case already count roots with multiplicity. \diamond*

We now discuss the number of roots, over a local field, of certain non-sparse univariate polynomials that nevertheless admit a compact expression, e.g., $(x_1^9 + 1)^{1000} - (x_1 - 3)^{2^8}$. We also discuss connections to the **P** vs. **NP** Problem. As we will see shortly, complexity theory leads us to challenging open problems that can be stated entirely within the context of arithmetic geometry.

1.2. Applications and New Conjectures on Straight-Line Programs.

A very natural notion refining sparsity (a.k.a. lacunarity) is *straight-line program (SLP) complexity*: it is simply a measure — more refined than counting monomials — of how complicated an algebraic expression is.

Definition 1.8. *For any $f \in \mathbb{Z}[x_1]$ let $\tau(f)$ — the SLP complexity of f — denote the smallest n such that $f = f_n$ identically where the sequence $(f_{-1}, f_0, f_1, \dots, f_n)$ satisfies the following conditions: $f_{-1} := 1$, $f_0 := x_1$, and, for all $i \geq 1$, f_i is a sum, difference, or product of some pair of elements (f_j, f_k) with $j, k < i$. \diamond*

The SLP complexity of f is clearly no more than the number of monomial terms of f and is often dramatically smaller. However, computing $\tau(f)$ exactly appears to be quite difficult

[GK96]. More to the point, relating SLP complexity to the number of roots of polynomials provides a delightfully direct way to go from the theory of sparse polynomials to deep open questions in complexity theory.

Theorem 1.3. (See [BCSS98, Thm. 3, Pg. 127] and [Bür09, Thm. 1.1].) *Suppose there is an absolute constant c such that for all nonzero $f \in \mathbb{Z}[x_1]$, the number of distinct roots of f in \mathbb{Z} is no more than $(\tau(f) + 1)^c$. Then $\mathbf{P}_{\mathbb{C}} \neq \mathbf{NP}_{\mathbb{C}}$, and the permanent of $n \times n$ matrices cannot be computed by constant-free, division-free arithmetic circuits of size polynomial in n . ■*

The hypothesis of the theorem is known as the **(Standard) τ -Conjecture**, and was also stated as the fourth problem on Smale's list of the most important problems for the 21st century [Sma98, Sma00].

Remark 1.9. *It turns out that upper bounds on $\Omega_L(n, k)$, for general n and k , and any field $L \supset \mathbb{Z}$, lead directly to upper bounds on the number of roots of $f \in \mathbb{Z}[x_1]$ in \mathbb{Z} as a function of $\tau(f)$. This was pursued earlier in [Gri82, Ris85, Roj02]. Unfortunately, the best current upper bounds on $\Omega_L(n, k)$ are not yet strong enough to yield the τ -Conjecture in this way. \diamond*

The complexity classes $\mathbf{P}_{\mathbb{C}}$ and $\mathbf{NP}_{\mathbb{C}}$ are respective analogues of the well-known complexity classes \mathbf{P} and \mathbf{NP} [BCSS98, AB09]. Just as in the famous \mathbf{P} vs. \mathbf{NP} Problem, the question $\mathbf{P}_{\mathbb{C}} \stackrel{?}{=} \mathbf{NP}_{\mathbb{C}}$ also remains open. Furthermore, the truth of $\mathbf{P}_{\mathbb{C}} = \mathbf{NP}_{\mathbb{C}}$ would imply collapses of complexity classes closely related to the \mathbf{P} vs. \mathbf{NP} Problem.³ The implications of $\mathbf{P}_{\mathbb{C}} \neq \mathbf{NP}_{\mathbb{C}}$ for classical complexity are not yet clear. However, there are number-theoretic results showing that if both the Generalized Riemann Hypothesis and $\mathbf{P}_{\mathbb{C}} \neq \mathbf{NP}_{\mathbb{C}}$ were true, then there would be some evidence that $\mathbf{P} \neq \mathbf{NP}$ [Koi96, Roj03b].

The assertion on the hardness of the permanent in Theorem 1.3 is also an open problem and its proof would be an important step toward solving the \mathbf{VP} vs. \mathbf{VNP} Problem. The latter problem is Valiant's circuit complexity analogue of the \mathbf{P} vs. \mathbf{NP} Problem and involves the choice of a ground field L [Val79, BLMW11]. Like the assertion $\mathbf{P}_{\mathbb{C}} = \mathbf{NP}_{\mathbb{C}}$, the truth of $\mathbf{VP}_L = \mathbf{VNP}_L$ (over certain fields L) would also imply a widely-doubted collapse of complexity classes. (See [Bür00] for further details.)

One natural approach to the τ -Conjecture would be to broaden it to inspire a new set of techniques, or rule out overly optimistic extensions. For instance, one might suspect that the number of roots of f in a field L containing \mathbb{Z} could also be polynomial in $\tau(f)$, thus allowing us to consider techniques applicable to L .

For L a number field, the truth of such an extension of the τ -Conjecture expands the list of its implications into arithmetic geometry. For instance, assuming an extension of the τ -Conjecture suitably bounding the number of degree d factors of a univariate polynomial over a number field L , one would be able to derive upper bounds for the number of torsion points on an elliptic curve E over L depending only on the field extension degree $[L : \mathbb{Q}]$. The resulting torsion bound proof would be dramatically simpler, and lead to bounds sharper than those derived in the famous works [Mer96, Par99]. In a different direction, Bürgisser has also studied the connections between similar extensions of the τ -Conjecture and polynomial factorization [Bür04]. However, the truth of any global field analogue of the τ -Conjecture remains unknown.

³ For the experts, the precise implication is $\mathbf{P}_{\mathbb{C}} = \mathbf{NP}_{\mathbb{C}} \implies \mathbf{NP} \subseteq \mathbf{BPP}$ [Shu93].

Over local fields, more is known, but the results are unfortunately negative: First, the case $L = \mathbb{R}$ breaks down rather quickly.

Example 1.10. Consider the recurrence $h_{n+1} := 4h_n(1 - h_n)$ (for all $n \geq 1$) with $h_1 := 4x_1(1 - x_1)$. Note that h_1 defines a degree 2 surjection from $[0, 1]$ to itself, ramified at $1/2$. It is then easily checked⁴ that $h_n(x_1) - x_1$ has degree 2^n , exactly 2^n roots in the open interval $(0, 1)$, and $\tau(h_n(x_1) - x_1) = O(n)$. Note, however, that $h_n(x_1) - x_1$ has no integer roots. \diamond

One could instead try the case $L \supseteq \mathbb{Q}_p$. Unfortunately, as pointed out to the author by Bjorn Poonen during a conversation at the Extensions of Hilbert's Tenth Problem workshop at the American Institute of Mathematics (March 21–25, 2005), there also exist p -adic analogues of the last example. Inspired by Poonen's construction over any particular \mathbb{Q}_p , we later derived the following example having “too many” roots over several \mathbb{Q}_p at once (see Section 3.4 for the proof).

Lemma 1.11. Let $k \geq 1$, $c_k := 2 \cdot 3 \cdot 5 \cdots p_k$ where p_k denotes the k^{th} prime, and consider the recurrence satisfying $h_{1,k} := x_1(1 - x_1)$ and $h_{n+1,k} := (c_k^{3^{n-1}} - h_{n,k})h_{n,k}$ for all $n \geq 1$. Then $\frac{h_{n,k}(x_1)}{x_1(1-x_1)} \in \mathbb{Z}[x_1]$ has degree $2^n - 2$, exactly $2^n - 2$ roots in \mathbb{Z}_p for each $p \in \{2, 3, 5, \dots, p_k\}$, and $\tau\left(\frac{h_{n,k}(x_1)}{x_1(1-x_1)}\right) = O(n + k(\log k)^2)$. However, $\frac{h_{n,k}(x_1)}{x_1(1-x_1)}$ has no real roots (and thus no integer roots).

Note that the two preceding families of extremal examples were of a very particular recursive form and had no integer roots at all. We are unaware if, over a non-algebraically closed local field, having a number of roots exponential in τ is in fact a rarity among the polynomials $f \in \mathbb{Z}[x_1]$ having $\tau(f) = \tau$. Note also that $\tau(h_{n,k}) \rightarrow \infty$ as $k \rightarrow \infty$ and $h_{n,k}$ begins to have roots in \mathbb{Q}_p for an increasing number of primes p . We are unaware if f having many roots — over many \mathbb{Q}_p simultaneously — actually forces $\tau(f)$ to be large. We point out, however, that it is possible for a univariate polynomial to have roots in \mathbb{R} , and \mathbb{Q}_p for all primes p , but no roots in \mathbb{Q} : $(x_1^2 - 2)(x_1^2 - 17)(x_1^2 - 34)$ [Kat07, Pg. 47, Ex. 46] is one of the simplest such examples.

Considering our preceding counter-examples and observations, we propose the following generalization of the τ -Conjecture.

Adelic τ -Conjecture. There is an absolute constant c such that, for any $f \in \mathbb{Z}[x_1]$, there is a field $L \in \{\mathbb{R}, \mathbb{Q}_2, \mathbb{Q}_3, \mathbb{Q}_5, \dots\}$ such that f has no more than $(\tau(f) + 1)^c$ roots in L .

The Adelic τ -Conjecture clearly implies the Standard τ -Conjecture and, so far, has no counter-examples.

To conclude our discussion of SLP complexity, we point out that Pascal Koiran has proved that the truth of weaker versions of the τ -Conjecture would still have major implications in complexity theory (see, e.g., [Koi10, Conj. 1 & Prop. 2]). Koiran has also suggested that such conjectural bounds be considered over the real numbers to enable the use of real analytic techniques. Our development here is thus a step toward including p -adic techniques as well.

⁴ This example is well-known in dynamical systems and was first pointed out to the author by Gregorio Malajovich some time before 2000. Similar examples also appeared in [BC76].

2. BACKGROUND: FROM TRIANGLES TO TORIC DEFORMATIONS

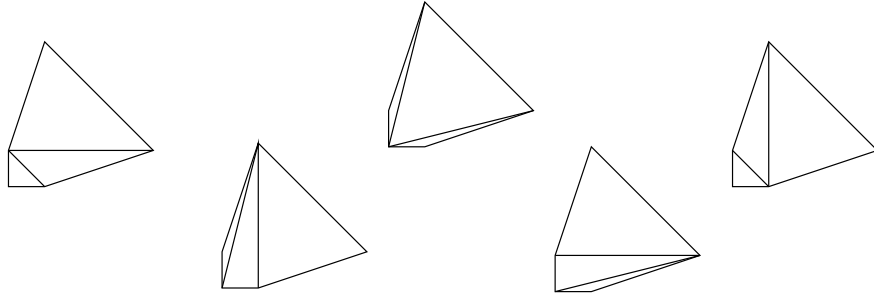
The key technique behind our fewnomial lower bounds is a polyhedral construction (Lemma 2.6 below) with several useful algebraic consequences.

Recall that a *triangulation* of a point set $\mathcal{A} \subset \mathbb{R}^n$ is simply a simplicial complex Σ whose vertices all lie in \mathcal{A} . Recall also that a *polyhedral subdivision* of a polytope Q is a collection of polytopes $\{C_i\}$ such that $\bigcup_i C_i = Q$ and, for all i and j , $C_i \cap C_j$ is a face of both C_i and C_j . Let $\text{Conv} S$ denote the convex hull of a point set S . We then say that a triangulation of \mathcal{A} is *coherent* iff its simplices are exactly the domains of linearity for some function $\ell : \text{Conv} \mathcal{A} \rightarrow \mathbb{R}$ that is convex, continuous, and piecewise linear. Such a function is called a *lifting* for \mathcal{A} (or a lifting for $\text{Conv} \mathcal{A}$), and we let $\hat{\mathcal{A}} := \{(a, \ell(a)) \mid a \in \mathcal{A}\}$. Abusing notation slightly, we also refer to $\hat{\mathcal{A}}$ as a *lifting of \mathcal{A} (with respect to ℓ)*.

Remark 2.1. *It follows directly from our last definition that a lifting function ℓ on $\text{Conv} \mathcal{A}$ is uniquely determined by the values of ℓ on \mathcal{A} . So we will henceforth specify such ℓ by specifying just the restricted image $\ell(\mathcal{A})$. \diamond*

Recall also that $\text{Supp}(f)$ denotes the set of exponent vectors (a.k.a. the *support* or *spectrum*) of f .

Example 2.2. *Consider $f(x) := 1 - x_1 - x_2 + \frac{6}{5}(x_1^4 x_2 + x_1 x_2^4)$. Then $\text{Supp}(f) = \{(0, 0), (1, 0), (0, 1), (1, 4), (4, 1)\}$ and has convex hull a pentagon. It is then easily checked that there are exactly 5 possible coherent triangulations for $\text{Supp}(f)$:*



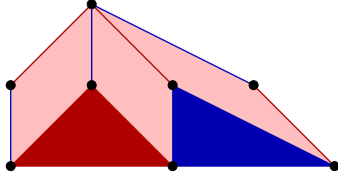
\diamond

Definition 2.3. (See also [HS95].) Recall that, for any polytope $\hat{Q} \subset \mathbb{R}^{n+1}$, we call a face \hat{P} of \hat{Q} a *lower face* iff \hat{P} has an inner normal with positive $(n+1)^{\text{st}}$ coordinate. Letting $\pi : \mathbb{R}^{n+1} \rightarrow \mathbb{R}^n$ denote the natural projection forgetting the last coordinate, the lower facets of \hat{Q} thus induce a natural polyhedral subdivision Σ of $Q := \pi(\hat{Q})$. In particular, if $\hat{Q} \subset \mathbb{R}^{n+1}$ is a Minkowski sum of the form $\hat{Q}_1 + \cdots + \hat{Q}_n$ where the \hat{Q}_i are polytopes of dimension $\leq n+1$, \hat{E}_i is a lower edge of \hat{Q}_i for all i , and $\hat{P} = \hat{E}_1 + \cdots + \hat{E}_n$ is a lower facet of \hat{Q} , then we call \hat{P} a *mixed lower facet* of \hat{Q} . Also, the resulting cell $\pi(\hat{P}) = \pi(\hat{E}_1) + \cdots + \pi(\hat{E}_n)$ of Σ is called a *mixed cell* of Σ . \diamond

Example 2.4. Let us consider the family of systems G_ε from Theorem 1.2 for $n = 2$. In particular, let $(\mathcal{A}_1, \mathcal{A}_2)$ be the pair of supports of G_ε , and let (Q_1, Q_2) be the corresponding pair of convex hulls in \mathbb{R}^2 . Let us also define a pair of liftings (ℓ_1, ℓ_2) via the exponents of the powers of ε appearing in the corresponding monomial terms, i.e., let us define

$$\begin{array}{ll} (0, 0) \mapsto 1 & (0, 0) \mapsto 0 \\ \ell_1 : (2, 0) \mapsto 0 & \ell_2 : (2, 0) \mapsto 1. \\ (1, 1) \mapsto 0 & (0, 1) \mapsto 0 \end{array}$$

These lifting functions then affect the shape of the lower hull of the Minkowski sum $\hat{Q}_1 + \hat{Q}_2$ of lifted polygons, which in turn fixes a subdivision Σ_{ℓ_1, ℓ_2} of $Q_1 + Q_2$ via the images of the lower facets of $\hat{Q}_1 + \hat{Q}_2$ under π . (See the illustration below.) In particular, the mixed cells of Σ_{ℓ_1, ℓ_2} ,



for this particular lifting, correspond to the lighter (pink) parallelograms: from left to right, they are exactly $E_{1,0} + E_{2,0}$, $E_{1,1} + E_{2,0}$, and $E_{1,1} + E_{2,1}$, where $E_{1,s}$ (resp. $E_{2,s}$) is an edge of Q_1 (resp. Q_2) for all s . More precisely, $E_{1,0}$, $E_{1,1}$, $E_{2,0}$,

and $E_{2,1}$ are respectively the convex hulls of $\{(0,0), (1,1)\}$, $\{(1,1), (2,0)\}$, $\{(0,0), (0,1)\}$, and $\{(0,1), (2,0)\}$. Note also that these mixed cells, through their expression as edges sums (and the obvious correspondence between vertices and monomial terms), correspond naturally to three binomial systems. In order, they are $(x_1x_2 - \varepsilon, x_2 - 1)$, $(x_1x_2 - x_1^2, x_2 - 1)$, and $(x_1x_2 - x_1^2, x_2 - \varepsilon x_1^2)$. In particular, the first (resp. second) polynomial of each such pair is a sub-sum of the first (resp. second) polynomial of G_ε . \diamond

Definition 2.5. (See also [HS95, Ewa96, Roj03a].) Let $\mathcal{A}_1, \dots, \mathcal{A}_n \subset \mathbb{R}^n$ be finite point sets with respective convex hulls Q_1, \dots, Q_n . Also let ℓ_1, \dots, ℓ_n be respective lifting functions for $\mathcal{A}_1, \dots, \mathcal{A}_n$ and consider the polyhedral subdivision $\Sigma_{\ell_1, \dots, \ell_n}$ of $Q := Q_1 + \dots + Q_n$ obtained via the images of the lower facets of \hat{Q} under π . In particular, if $\dim \hat{P}_1 + \dots + \dim \hat{P}_n = n$ for every lower facet of \hat{Q} of the form $\hat{P}_1 + \dots + \hat{P}_n$, then we say that (ℓ_1, \dots, ℓ_n) is mixed. For any such n -tuple of liftings we then define the mixed volume of (Q_1, \dots, Q_n) to be

$$\mathcal{M}(Q_1, \dots, Q_n) := \sum_{\substack{C \text{ a mixed cell} \\ \text{of } \Sigma_{\ell_1, \dots, \ell_n}}} \text{Vol}(C),$$

following the notation of Definition 2.3. \diamond

As an example, the mixed volume of the two triangles from Example 2.4, relative to the stated lifting, is the sum of the areas of the three parallelograms in the illustration, i.e., 3. The preceding definition is in fact independent of the liftings ℓ_1, \dots, ℓ_n , and is so far the most computationally practical [HS95, DGH98].

Theorem 2.1. (See, e.g., [Ewa96, Ch. IV, pg. 126].) The formula for $\mathcal{M}(Q_1, \dots, Q_n)$ from Definition 2.5 is independent of the underlying mixed n -tuple of liftings (ℓ_1, \dots, ℓ_n) . Furthermore, if $Q'_1, \dots, Q'_n \subseteq \mathbb{R}^n$ are any polytopes with $Q'_i \supseteq Q_i$ for all i , then $\mathcal{M}(Q_1, \dots, Q_n) \leq \mathcal{M}(Q'_1, \dots, Q'_n)$. Finally, the n -dimensional mixed volume satisfies $\mathcal{M}(Q, \dots, Q) = n! \text{Vol}(Q)$ for any polytope $Q \subset \mathbb{R}^n$. \blacksquare

Lemma 2.6. Let $n \geq 2$, and let \mathbf{O} and e_i respectively denote the origin and i^{th} standard basis vector in \mathbb{R}^{n+1} . Consider the triangles

$$\begin{aligned} \hat{T}_1 &:= \text{Conv}\{e_{n+1}, 2e_1, e_1 + e_2\} \\ \hat{T}_2 &:= \text{Conv}\{\mathbf{O}, 2e_1 + e_{n+1}, e_2 + e_3\} \\ \hat{T}_3 &:= \text{Conv}\{\mathbf{O}, 2e_1 + 3e_{n+1}, e_3 + e_4\} \\ &\vdots \\ \hat{T}_{n-1} &:= \text{Conv}\{\mathbf{O}, 2e_1 + (2n-5)e_{n+1}, e_{n-1} + e_n\} \\ \hat{T}_n &:= \text{Conv}\{\mathbf{O}, 2e_1 + (2n-3)e_{n+1}, e_n\}. \end{aligned}$$

Then the Minkowski sum $\hat{T} := \hat{T}_1 + \dots + \hat{T}_n$ has exactly $n+1$ mixed lower facets. More precisely, for any $j \in \{0, \dots, n\}$, we can obtain a unique mixed lower facet,

$$\hat{P}_j := \hat{E}_{1,1} + \cdots + \hat{E}_{j,1} + \hat{E}_{j+1,0} + \cdots + \hat{E}_{n,0},$$

with $\text{Vol}(\pi(\hat{P}_j)) = 1$, in the following manner: for all $i \in \{1, \dots, n\}$, define $\hat{E}_{i,1}$ (resp. $\hat{E}_{i,0}$) to be the convex hull of the second (resp. first) and third listed vertices for \hat{T}_i . Finally, $\mathcal{M}(\pi(\hat{T}_1), \dots, \pi(\hat{T}_n)) = n+1$ and, for each $j \in \{0, \dots, n\}$, the vector

$$v_j := e_{n+1} + e_1 - \sum_{i=1}^j (j+1-i)e_i$$

is a nonzero inner normal for the lower facet \hat{P}_j .

Finding explicit coordinates yielding a collection of triangles $\hat{T}_1, \dots, \hat{T}_n \subset \mathbb{R}^{n+1}$ with the $\pi(\hat{T}_i)$ sharing a parallel edge and $\pi(\hat{T}_i)$ having enough mixed cells was challenging, involving numerous computational experiments. However, once one has the coordinates above, the proof of the lemma reduces to simply checking that each inner normal stated above evinces the corresponding mixed facet. The latter in turn reduces to a simple computation detailed in Section 3.3.

The next result we need is a beautiful generalization, by Bernd Sturmfels, of Viro's Theorem. Let us first review the relevant notation. We use ∂Q for the boundary of a polytope Q .

Definition 2.7. Suppose $\mathcal{A} \subset \mathbb{Z}^n$ is finite and $\text{Conv} \mathcal{A} > 0$. We call any function $s : \mathcal{A} \rightarrow \{\pm\}$ a distribution of signs for \mathcal{A} , and we call any pair (Σ, s) with Σ a coherent triangulation of \mathcal{A} a signed (coherent) triangulation of \mathcal{A} . We also call any edge of Σ with vertices of opposite sign an alternating edge.

Given a signed triangulation for \mathcal{A} we then define a piece-wise linear manifold — the Viro diagram $\mathcal{V}_{\mathcal{A}}(\Sigma, s)$ — in the following local manner: For any n -cell $C \in \Sigma$, let L_C be the convex hull of the set of midpoints of the alternating edges of C , and then define $\mathcal{V}_{\mathcal{A}}(\Sigma, s) := \bigcup_{\substack{C \text{ an } n\text{-cell} \\ \text{of } \Sigma}} L_C \setminus \partial \text{Conv}(\mathcal{A})$. Finally, when $\mathcal{A} = \text{Supp}(f)$ and s is the corresponding

sequence of coefficient signs, then we call $\mathcal{V}_{\Sigma}(f) := \mathcal{V}_{\mathcal{A}}(\Sigma, s)$ the Viro diagram of f . \diamond

Viro's Theorem (see, e.g., Proposition 5.2 and Theorem 5.6 of [GKZ94, Ch. 5, pp. 378–393] or [Vir84]) states that, under certain conditions, one may find a triangulation Σ with the positive zero set of f homeomorphic to $\mathcal{V}_{\Sigma}(f)$. Sturmfels' Theorem for Complete Intersections extends this to systems of equations, and we will need just the special case of $n \times n$ polynomial systems.

Definition 2.8. Suppose $\mathcal{A}_1, \dots, \mathcal{A}_n \subset \mathbb{Z}^n$ and each \mathcal{A}_i is endowed with a lifting ℓ_i and a distribution of signs s_i . Then, following the notation of Definition 2.5, we call a mixed cell $E_1 + \cdots + E_n$ of $\Sigma_{\ell_1, \dots, \ell_n}$ an alternating mixed cell of $(\Sigma_{\ell_1, \dots, \ell_n}, s_1, \dots, s_n)$ iff each edge E_i is alternating (as an edge of the triangulation of \mathcal{A}_i induced by ℓ_i). \diamond

Example 2.9. Returning to Example 2.4, it is clear that we can endow the supports of G_{ε} with the distribution of signs corresponding to the underlying coefficients. We then see that when $\varepsilon > 0$, each of the 3 mixed cells is alternating. \diamond

Sturmfels' Theorem for Complete Intersections (special case). [Stu94, Thm. 4] Suppose $\mathcal{A}_1, \dots, \mathcal{A}_n$ are finite subsets of \mathbb{Z}^n , $(c_{i,a} \mid i \in \{1, \dots, n\}, a \in \mathcal{A}_i)$ is any vector of nonzero real numbers, and (ℓ_1, \dots, ℓ_n) is a mixed n -tuple of lifting functions for $\mathcal{A}_1, \dots, \mathcal{A}_n$.

Let $\Sigma_{\ell_1, \dots, \ell_n}$ denote the resulting polyhedral subdivision of $\text{Conv}(\mathcal{A}_1) + \dots + \text{Conv}(\mathcal{A}_n)$ (as in Definition 2.5) and let $s_i := (\text{sign}(c_{i,a}) \mid a \in \mathcal{A}_i)$ for all i . Then, for all $t > 0$ sufficiently small, the system of equations

$$\begin{aligned} \sum_{a \in \mathcal{A}_1} c_{1,a} t^{\ell_1(a)} x^a \\ \vdots \\ \sum_{a \in \mathcal{A}_n} c_{n,a} t^{\ell_n(a)} x^a \end{aligned}$$

has exactly N roots in \mathbb{R}_+^n , where N is the number of alternating cells of $(\Sigma_{\ell_1, \dots, \ell_n}, s_1, \dots, s_n)$. ■

A final tool we'll need is the non-Archimedean Newton polytope, along with a recent refinement incorporating generalized phase.

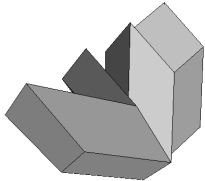
Definition 2.10. Given any non-Archimedean local field L with uniformizing parameter ρ , and any Laurent polynomial $f(x) := \sum_{i=1}^m c_i x^{a_i} \in L[x_1^{\pm 1}, \dots, x_n^{\pm 1}]$, we define its non-Archimedean Newton polytope to be $\text{Newt}_\rho(f) := \text{Conv}\{(a_i, \text{ord } c_i) \mid i \in \{1, \dots, m\}\}$. Also, the polynomial associated to summing the terms of f corresponding to points of the form $(a_i, \text{ord } c_i)$ lying on a lower face of $\text{Newt}_\rho(f)$ is called a lower polynomial. ◇

Note that ρ is a generator of the maximal ideal \mathfrak{M} so it will make sense to speak of Newt_ρ and Newt_t , depending on the context.

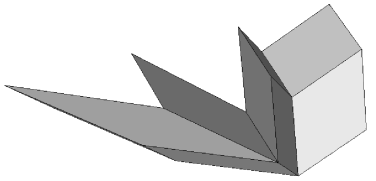
A remarkable fact true over non-Archimedean algebraically closed fields but false over \mathbb{C} is that the norms of roots of polynomials can be determined completely combinatorially. What is less well-known is that, under certain conditions, the generalized phases of the roots can also be found by simply solving some lower binomial systems.

Theorem 2.2. (See [AI11, Thm. 3.10 & Prop. 4.4].) Suppose L is a non-Archimedean local field, $f_1, \dots, f_n \in L[x_1^{\pm 1}, \dots, x_n^{\pm 1}]$, and $(v, 1)$ is an inner normal to a mixed lower facet of the form $\hat{E} := \hat{E}_1 + \dots + \hat{E}_n$ where \hat{E}_i is a lower edge of $\text{Newt}_\rho(f_i)$ for all i . Suppose also that the lower polynomials g_1, \dots, g_n corresponding to the normal $(v, 1)$ are all binomials, and that $\pi(\hat{E})$ has standard Euclidean volume 1. Then the number of roots $\zeta \in L^n$ of $F := (f_1, \dots, f_n)$ with $\text{ord } \zeta = v$ and generalized phase θ is exactly the number of roots of (g_1, \dots, g_n) in L^n with $\text{ord } \zeta = v$ and generalized phase θ , for any vector $\theta = (\theta_1, \dots, \theta_n)$ with nonzero coordinates in the residue field of L . ■

Example 2.11. Let $p \in \mathbb{N}$ be any prime, $n=3$, and let $(\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3)$ be the triple of supports for the system G_p (see Theorem 1.2). Also let ℓ_1, ℓ_2, ℓ_3 be the respective liftings obtained by using the p -adic valuations of the coefficients of G_p . Then $(\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3)$ has exactly 4 mixed cells, two views of which are shown below. The corresponding lower binomial systems are shown as well:



$x_1 x_2 - p$	$x_1 x_2 - x_1^2$	$x_1 x_2 - x_1^2$	$x_1 x_2 - x_1^2$
$x_2 x_3 - 1$	$x_2 x_3 - 1$	$x_2 x_3 - p x_1^2$	$x_2 x_3 - p x_1^2$
$x_3 - 1$	$x_3 - 1$	$x_3 - 1$	$x_3 - p^3 x_1^2$



Each mixed cell has volume 1, and each corresponding binomial system has a unique solution in $(\mathbb{Q}_p^*)^3$. In order, the solutions are $(p, 1, 1)$, $(1, 1, 1)$, $(p^{-1}, p^{-1}, 1)$, (p^{-2}, p^{-2}, p^{-1}) . It then follows immediately from Theorem 2.2 that G_p has roots in $(\mathbb{Q}_p^*)^3$ of the form:

$$(p(1 + O(p)), 1 + O(p), 1 + O(p)), \quad (1 + O(p), 1 + O(p), 1 + O(p)), \\ (p^{-1}(1 + O(p)), p^{-1}(1 + O(p)), 1 + O(p)), \text{ and } (p^{-2}(1 + O(p)), p^{-2}(1 + O(p)), p^{-1}(1 + O(p))). \quad \diamond$$

3. PROVING OUR MAIN RESULTS

3.1. Theorem 1.1: The Universal Lower Bound.

The lower bound $\Omega_L(1, k) \geq k$ is easily evinced over the fields \mathbb{R} , \mathbb{Q}_p , and $\mathbb{F}_p((t))$ respectively by the polynomials $(x_1 - 1) \cdots (x_1 - k)$, $(x_1 - 1) \cdots (x_1 - p^{k-1})$, and $(x_1 - 1) \cdots (x_1 - t^{k-1})$. (Proposition 1.4 reveals an even better lower bound in the positive characteristic case but this need not concern us here.) So let us assume $n \geq 2$.

The Archimedean case then follows easily from [LRW03, Thm. 4] (for $n \leq k - 1$) and [BRS07, Thm. 1] (for $n > k - 1$). In the non-Archimedean setting, the special case $n \leq k - 1$ follows easily from [Roj04, Example 2]. So it suffices to prove the special case $n > k - 1$ in the non-Archimedean setting. We may also assume $k \geq 2$ since we already know from the introduction that $\Omega_L(n, 1) = 1$.

Let us assume temporarily that $\Omega_L(n, 2) \geq n + 1$ for all n , and see how this enables us to construct an $n \times n$ $(n + k)$ -nomial system with at least $\lfloor \frac{n+k-1}{k-1} \rfloor^{k-1}$ non-degenerate roots in L^n with all coordinates having generalized phase 1: First, letting $\ell := \lfloor \frac{n}{k-1} \rfloor$, we can clearly write $n = (k - 1)\ell + m$ with $m \in \{0, \dots, k - 2\}$. By assumption, there is then an $\ell \times \ell$ $(\ell + 2)$ -nomial system (g_1, \dots, g_ℓ) with at least $\ell + 1$ non-degenerate roots in L^ℓ with all coordinates having generalized phase 1. (By dividing all the g_i by some suitable monomial, we may also assume that some g_j has a constant term.) So then consider the new system

$$\begin{aligned} x_{0,1} - 1 &= 0 \\ &\vdots \\ x_{0,m} - 1 &= 0 \\ g_1(x_{1,1}, \dots, x_{1,\ell}) &= \cdots = g_\ell(x_{1,1}, \dots, x_{1,\ell}) = 0 \\ &\vdots \\ g_1(x_{k-1,1}, \dots, x_{k-1,\ell}) &= \cdots = g_\ell(x_{k-1,1}, \dots, x_{k-1,\ell}) = 0 \end{aligned}$$

Clearly, this new system consists of $n = (k - 1)\ell + m$ polynomials in $n = (k - 1)\ell + m$ variables. Furthermore, the number of distinct exponent vectors is clearly $\leq 1 + m + (k - 1)(\ell + 1) = n + k$. Finally, the number of non-degenerate roots in L^n , with coordinates all having generalized phase 1, is clearly at least $(\ell + 1)^{k-1} = (\lfloor \frac{n}{k-1} \rfloor + 1)^{k-1} = \lfloor \frac{n+k-1}{k-1} \rfloor^{k-1}$.

So now we need only show that $\Omega_L(n, 2) \geq n + 1$. This follows immediately from Theorem 1.2. ■

3.2. Theorem 1.2: Universal Extremal Systems Supported on Circuits.

First note that all the roots of G_ε in \bar{L}^n lie in $(\bar{L}^*)^n$. (Clearly, setting any $x_i = 0$ results in a pair of univariate polynomials having no roots in common, or a nonzero constant being equal to zero.) Let $(g_1, \dots, g_n) := G_\varepsilon$ and let \mathcal{A} denote the matrix whose columns are the union of the supports of the g_i . More precisely, let us set \mathcal{A} to be the $n \times (n + 2)$ matrix

$$\begin{bmatrix} 0 & 2 & 1 & 0 & & & & & \\ & & 1 & 1 & & & & & \\ & & & 1 & & & & & \\ & & & & \ddots & & & & \\ & & & & & 1 & & & \\ & & & & & 1 & 1 & & \end{bmatrix}$$

Let $\bar{\mathcal{A}}$ denote the $(n + 1) \times (n + 2)$ matrix obtained by appending a row of 1s to the top of \mathcal{A} . It is then easily checked that $\bar{\mathcal{A}}$ has right null-space of dimension 1, generated by the transpose of $b := (b_1, \dots, b_{n+2}) = (-1, (-1)^n, (-1)^{n+1}2, \dots, (-1)^{n+n}2)$. We can then rewrite the equation $g_i = 0$ as $x^{a_i+2} = \beta_i(x_1^2)$, where a_i denotes the i^{th} column of \mathcal{A} and β_i is a suitable degree one polynomial with coefficients that are powers of ε .

Since the entries of b sum to 0, we then easily obtain that

$$1^{b_1} u^{b_2} \beta_1(u)^{b_3} \cdots \beta_n(u)^{b_{n+2}} = 1$$

when $\zeta = (\zeta_1, \dots, \zeta_n)$ is a root of G_ε in \bar{L}^n and $u := \zeta_1^2$. In other words, the degree $n + 1$ polynomial

$$\begin{aligned} R_n(u) &:= u\beta_2(u)^2\beta_4(u)^2 \cdots \beta_{2\lfloor n/2 \rfloor}(u)^2 - \beta_1(u)^2\beta_3(u)^2 \cdots \beta_{2\lceil n/2 \rceil-1}(u)^2 \\ &= u(1+\varepsilon u)^2(1+\varepsilon^5 u)^2 \cdots (1+\varepsilon^{4\lfloor n/2 \rfloor-3} u)^2 - (\varepsilon+u)^2(1+\varepsilon^3 u)^2(1+\varepsilon^7 u)^2 \cdots (1+\varepsilon^{4\lceil n/2 \rceil-5} u)^2 \end{aligned}$$

must vanish. There are thus no more than $n + 1$ possible values for u in \bar{L} . Furthermore, the value of ζ_n is uniquely determined by the value of u , thanks to the equation $g_n = 0$. Proceeding with the remaining equations $g_{n-1} = 0, \dots, g_1 = 0$ we see that the same holds for $\zeta_{n-1}, \dots, \zeta_2$ and ζ_1 successively. So G_ε has no more than $n + 1$ roots, counting multiplicities, in \bar{L}^n . Note in particular that by Lemma 2.6, combined with Bernstein's Theorem [Dan78, Ful93, Roj03a], G_ε having at least $n + 1$ distinct roots in \bar{L}^n implies that there are *exactly* $n + 1$ roots in \bar{L}^n and they are all non-degenerate.

To prove the remainder of our theorem, we separate the Archimedean and non-Archimedean cases: when $\mathcal{L} = \mathbb{R}$, we immediately obtain from Lemma 2.6 and Sturm's Theorem that G_ε has at least $n + 1$ positive roots. For the non-Archimedean case, Lemma 2.6 and Theorem 2.2 immediately imply that G_ε has at least $n + 1$ roots in L^n with all coordinates having generalized phase 1. In particular, writing $v_j = (v_{1,j}, \dots, v_{n,j}, 1)$, it is easily checked that $(p^{v_{1,j}}, \dots, p^{v_{n,j}})$ is a solution of the corresponding lower binomial system of G_ε .

The only assertion left to prove is that $\varepsilon = 1/4$ is small enough (for the roots of G_ε to behave as claimed) for $n \in \{2, \dots, 100\}$. This was done via the `realroot` command (in `Maple14`) applied directly to the polynomial $R_n(u)$ and took less than 1 hour. ■

3.3. The Proof of Lemma 2.6. Let us first prove that the stated mixed volume is at most $n + 1$: by Theorem 2.1 our mixed volume in question is bounded above by $n! \text{Vol}(Q)$ where Q is the polytope with vertices the columns of the matrix \mathcal{A} from the proof of Theorem 1.2. The vertices of Q form a *circuit* and the signs of the entries of the vector b from the proof of Theorem 2.1, thereby encode an explicit triangulation of Q (see, e.g., [GKZ94, Prop. 1.2, pg. 217]). More precisely, defining $Q(i)$ to be the convex hull of the points corresponding to all the columns of \mathcal{A} *except* for the i^{th} column, we obtain that $\{Q(2), Q(4), \dots, Q(2 \lfloor \frac{n+2}{2} \rfloor)\}$ (for n even), and $\{Q(3), Q(5), \dots, Q(2 \lceil \frac{n+2}{2} \rceil - 1)\}$ (for n odd), forms the simplices of a triangulation of Q . Note in particular that the volume of $Q(i)$ is exactly $1/n!$ times the absolute value of the determinant of the submatrix of \mathcal{A} obtained by deleting the first and i^{th} columns. Note also that this submatrix is block-diagonal with exactly 2 blocks: an $(i-2) \times (i-2)$ upper-left upper-triangular block and an $(n-i+2) \times (n-i+2)$ lower-right lower-triangular block. It is then clear that $\text{Vol}(Q(i))$ is 1 or 2, according as $i = 2$ or $i \geq 3$. So $\text{Vol}(Q)$ is then $1 + 2(\lfloor \frac{n+2}{2} \rfloor - 1) = n + 1$ (when n is even) or $2(\lceil \frac{n+2}{2} \rceil - 1) = n + 1$ (when n is odd).

We now observe that each cell $\pi(\hat{P}_j)$ has positive volume: this follows immediately from the fact that any n -tuple of columns chosen from the last $n + 1$ columns of \mathcal{A} is linearly independent. (The latter fact follows directly from our preceding block diagonal characterization of certain submatrices of \mathcal{A} .) In particular, once we show that each such cell is distinct, we immediately obtain that our mixed volume is at least $n + 1$ and thus equal to $n + 1$. So let us now check that each v_j is indeed an inner normal to \hat{P}_j .

For any $i \in \{1, \dots, n\}$ let $\hat{\mathcal{A}}_i = (\alpha_i, \beta_i, \gamma_i)$ denote the triple of vertices of the triangle \hat{T}_i , ordered so that $\pi(\alpha_i) = \mathbf{0}$ and $\pi(\beta_i) = 2e_1$. It then clearly suffices to prove that, for any $j \in \{0, \dots, n\}$, the inner product $v_j \cdot x$ is minimized on each $\hat{\mathcal{A}}_i$ exactly at the vertices of the edge $\hat{E}_{i,s}$, where s is 1 or 0 according as $i \leq j$ or $i \geq j+1$. Equivalently, this means that the minimum values in the triple $(v_j \cdot \alpha_i, v_j \cdot \beta_i, v_j \cdot \gamma_i)$ must occur exactly at the second and third (resp. first and third) coordinates when $i \leq j$ (resp. $i \geq j+1$).

Direct computation then reveals that $(v_0 \cdot \alpha_1, v_0 \cdot \beta_1, v_0 \cdot \gamma_1) = (1, 2, 1)$ and, for all $j \in \{1, \dots, n\}$, we have $(v_j \cdot \alpha_1, v_j \cdot \beta_1, v_j \cdot \gamma_1) = (1, 2-2j, 2-2j)$. For $i=0$, we thus see that the minima indeed occur at the prescribed coordinates.

So we may assume $i \geq 2$. More direct evaluation then yields $(v_0 \cdot \alpha_i, v_0 \cdot \beta_i, v_0 \cdot \gamma_i) = (0, 2i-1, 0)$ and $(v_1 \cdot \alpha_i, v_1 \cdot \beta_i, v_1 \cdot \gamma_i) = (0, 2i-3, 0)$. Again, we thus see that the minima indeed occur at the prescribed coordinates.

So we may now assume that $j \geq 2$ (as well as $i \geq 2$). It is then clear that $v_j \cdot \alpha_i = 0$ and $v_j \cdot \beta_i = (1-j) \cdot 2 + 1 \cdot (2i-3) = 2(i-j) - 1$.

Now, when $i \leq j-1$, we also obtain that $v_j \cdot \gamma_i = -(j+1-i) - (j+1-(i+1)) = 2(i-j) - 1$. Similarly, when $i = j$, we see that $v_j \cdot \gamma_i = -(j+1-i) = -1$ which still agrees with $v_j \cdot \beta_i$ in this case. So, when $i \leq j$, we see that the minimum of $(v_j \cdot \alpha_i, v_j \cdot \beta_i, v_j \cdot \gamma_i)$ occurs exactly at the second and third coordinates.

To conclude, observe that when $i \geq j+1$, $v_j \cdot \gamma_i = 0$ and $v_j \cdot \beta_i \geq 1$. So the minimum of $(v_j \cdot \alpha_i, v_j \cdot \beta_i, v_j \cdot \gamma_i)$ occurs exactly at the first and third coordinates. So we are done. ■

3.4. The Proof of Lemma 1.11. The assertion on the degree of $\frac{h_{n,k}(x_1)}{x_1(1-x_1)}$ is obvious from the recurrence for $h_{n,k}$. The upper bound on $\tau\left(\frac{h_{n,k}(x_1)}{x_1(1-x_1)}\right)$ follows easily from classical facts on the distribution of primes and recursive squaring. More precisely, [BS96, Thm. 8.8.4, Pg. 233] tells us that $k \log k < p_k < k(\log k + \log \log k)$ for all $k \geq 6$. So then p_k has no more than $O(\log k)$ binary digits and, since $\tau(2^i) = O(i)$, we easily obtain $\tau(p_k) = O((\log k)^2)$ and $\tau(c_k) = O(k(\log k)^2)$. Expressing $c_k^{3^{n-1}} = (\dots (c_k^3)^3 \dots)^3$, it is then clear that $\tau\left(c_k^{3^{n-1}}\right) = O(n + k(\log k)^2)$. Observing that we can easily evaluate $\frac{h_{n,k}(x_1)}{x_1(1-x_1)}$ by simply replacing $h_{2,k}$ by $c_k - h_{1,k}$ in the recurrence for $h_{n,k}$, we arrive at our bound for $\tau\left(\frac{h_{n,k}(x_1)}{x_1(1-x_1)}\right)$. Note also that by construction, $\frac{h_{n,k}(x_1)}{x_1(1-x_1)}$ does not vanish at 0 or 1, but does vanish at every other root of $h_{n,k}$.

We now focus on counting the roots of $\frac{h_{n,k}(x_1)}{x_1(1-x_1)}$ in the rings \mathbb{Z}_p for $p \in \{2, 3, 5, \dots, p_k\}$. From our last observations, it clearly suffices to show that, for all $n \geq 1$, $h_{n,k}$ has exactly 2^n roots in \mathbb{Z}_p for each $p \in \{2, 3, 5, \dots, p_k\}$. We do this by induction, using the following refined induction hypothesis:

For any prime $p \in \{2, 3, \dots, p_k\}$, $h_{n,k}$ has exactly 2^n distinct roots in \mathbb{Z}_p .

Furthermore, these roots are distinct mod $p^{3^{n-1}}$ and, for any such root ζ , the p -adic valuation of $h'_{n,k}(\zeta)$ is $\frac{3^{n-1}-1}{2}$.

The case $n=1$ is clear, and one also observes that $h'_{1,k}(x_1) = 1 - 2x_1$. Furthermore, one sees that the recurrence $h'_{n+1,k} = (c_k^{3^{n-1}} - h_{n,k})h'_{n,k}$ holds. So let us now assume the induction hypothesis for any particular n and prove the case $n+1$. In particular, let $\zeta \in \mathbb{Z}_p$ be any of the 2^n roots of $h_{n,k}$. Note then that the derivatives of $h_{n,k}$ and $c_k^{3^{n-1}} - h_{n,k}$ differ only by sign mod $p^{3^{n-1}}$. So by Hensel's Lemma (combined with our induction hypothesis), $c_k^{3^{n-1}} - h_{n,k}$

also has 2^n distinct roots in \mathbb{Z}_p . However, the roots of $c_k^{3^{n-1}} - h_{n,k}$ in \mathbb{Z}_p are all distinct from the roots of $h_{n,k}$ in \mathbb{Z}_p : this is because $c_k^{3^{n-1}} - h_{n,k}$ is nonzero at every root of $h_{n,k}(x_1) \bmod p^{3^{n-1}+1}$. So $h_{n+1,k}$ then clearly has 2^{n+1} distinct roots in \mathbb{Z}_p , and these roots remain distinct mod p^{3^n} . Furthermore, by our recurrence for $h'_{n,k}$, the p -adic valuation of $h'_{n+1,k}$ is exactly $3^{n-1} + \frac{3^{n-1}-1}{2} = \frac{3^n-1}{2}$. So our induction is complete.

To see that $\frac{h_{n,k}(x_1)}{x_1(1-x_1)}$ has no real roots, first note that $x_1(1-x_1)$ is strictly increasing on $(-\infty, 1/2)$, strictly decreasing on $(1/2, +\infty)$, and attains a unique maximum of $1/4$ at $x_1 = 1/2$. Since $c_k \geq 2$, we also clearly obtain that $c_k - x_1(1-x_1)$ has range contained in $[3/4, +\infty)$, with minimum occurring at $x_1 = 1/2$. More generally, our recurrence for $h'_{n,k}$ implies that any critical point $\zeta \in \mathbb{R}$ of $h'_{n,k}$, other than a critical point of $h_{n-1,k}$, must satisfy $c_k^{3^{n-1}} = 2h_{n-1,k}(\zeta)$. So, in particular, $h_{2,k}$ has the same regions of strict increase and strict decrease as $h_{1,k}$, and thus $h_{2,k}$ has maximum $\leq 3/8$. Proceeding by induction, we see thus see that $h_{n,k}$ has no critical points other than $1/2$ and thus no real roots other than 0 and 1 . Moreover, the latter roots occur with multiplicity 1 from the obvious recursive factorization of $h_{n,k}$. So $\frac{h_{n,k}(x_1)}{x_1(1-x_1)}$ has no real roots. ■

ACKNOWLEDGEMENTS

I thank Matt Papanikolas, Bjorn Poonen, and Philippe Pébay for many useful discussions, some of them p -adic. I also thank Martin Avendaño for pointing out which of his results would yield Theorem 2.2.

I dedicate this paper in honor of Bernd Sturmfels' 50th birthday. Happy 50 Bernd!

REFERENCES

- [AB09] Arora, Sanjeev and Barak, Boaz, *Computational complexity. A modern approach*. Cambridge University Press, Cambridge, 2009.
- [Ave07] Avendaño, Martin, “The number of real roots of a bivariate polynomial on a line,” *Journal of Symbolic Computation* 44 (9), pp. 1280–1284 (2009).
- [AI10] Avendaño, Martin and Ibrahim, Ashraf, “Ultrametric root counting,” *Houston Journal of Mathematics*, vol. 36 (4), pp. 1011–1022, 2010.
- [AI11] Avendaño, Martin and Ibrahim, Ashraf, “Multivariate ultrametric root counting,” in *Randomization, Relaxation, and Complexity in Polynomial Equation Solving*, Contemporary Mathematics, vol. 556, pp. 1–24, AMS Press, 2011.
- [AK10] Avendaño, Martín and Krick, Teresa, “Sharp Bounds for the Number of Roots of Univariate Fewnomials,” submitted for publication. Also available as Math ArXiv preprint [arXiv:1008.4808](#).
- [BS96] Bach, Eric and Shallit, Jeff, *Algorithmic Number Theory, Vol. I: Efficient Algorithms*, MIT Press, Cambridge, MA, 1996.
- [Bih07] Bihan, Frederic, “Polynomial systems supported on circuits and dessins d’enfants,” *J. London Math. Soc.* 75 (2007), no. 1, pp. 116–132.
- [BS07] Bihan, Frederic and Sottile, Frank, “New Fewnomial Upper Bounds from Gale Dual Polynomial Systems,” *Moscow Mathematical Journal*, 7 (2007), no. 3, pp. 387–407.
- [BS09] Bates, Dan and Sottile, Frank, “Khovanskii-Rolle continuation for real solutions,” submitted for publication. Also available as Math ArXiv preprint [arXiv:0908.4579](#).
- [BRS07] Bihan, Frederic; Rojas, J. Maurice; and Sottile, Frank, “On the Sharpness of Fewnomial Bounds and the Number of Components of Fewnomial Hypersurfaces,” *IMA Volume 146: Algorithms in Algebraic Geometry* (edited by A. Dickenstein, F.-O. Schreyer, and A. J. Sommese), pp. 15–20, Springer, New York, 2007.

- [BRS09] Bihan, Frederic; Rojas, J. Maurice; Stella, Case E., “*Faster Real Feasibility via Circuit Discriminants*,” proceedings of International Symposium on Symbolic and Algebraic Computation (ISSAC 2009, July 28–31, Seoul, Korea), pp. 39–46, ACM Press, 2009.
- [BCSS98] Blum, Lenore; Cucker, Felipe; Shub, Mike; and Smale, Steve, *Complexity and Real Computation*, Springer-Verlag, 1998.
- [BC76] Borodin, Alan and Cook, Steve, “*On the number of additions to compute specific polynomials*,” SIAM Journal on Computing, 5(1):146–157, 1976.
- [Bür00] Bürgisser, Peter, “*Cook’s versus Valiant’s Hypothesis*,” Theor. Comp. Sci., 235:71–88, 2000.
- [Bür04] Bürgisser, Peter, “*The Complexity of Factors of Multivariate Polynomials*,” Found. Comput. Math. 369–396 (2004).
- [Bür09] ———, “*On defining integers and proving arithmetic circuit lower bounds*,” Computational Complexity, 18:81–103, 2009.
- [BLMW11] Bürgisser, Peter; Landsberg, J. M.; Manivel, Laurent; and Weyman, Jerzy, “*An Overview of Mathematical Issues Arising in the Geometric Complexity Theory Approach to $\mathbf{VP} \neq \mathbf{VNP}$* ,” SIAM J. Comput. **40**, pp. 1179–1209, 2011.
- [Che04] Cheng, Qi, “*Straight Line Programs and Torsion Points on Elliptic Curves*,” Computational Complexity, Vol. 12, no. 3–4 (sept. 2004), pp. 150–161.
- [CZ02] Cohen, Paula B. and Zannier, Umberto, “*Fewnomials and intersections of lines with real analytic subgroups in \mathbf{G}_m^n* ,” Bull. London Math. Soc. 34 (2002), no. 1, pp. 21–32.
- [Dan78] Danilov, V. I., “*The Geometry of Toric Varieties*,” Russian Mathematical Surveys, 33 (2), pp. 97–154, 1978.
- [DvdD88] Denef, Jan and van den Dries, Lou, “*p-adic and Real Subanalytic Sets*,” Annals of Mathematics (2) **128** (1988), no. 1, pp. 79–138.
- [DGH98] Dyer, Martin; Gritzmann, Peter; and Hufnagel, Alexander, “*On the Complexity of Computing Mixed Volumes*,” SIAM J. Comput. **27** (1998), no. 2, pp. 356–400.
- [Ewa96] Ewald, Günter, *Combinatorial Convexity and Algebraic Geometry*, Graduate Texts in Mathematics 168, Springer-Verlag, New York, 1996.
- [Ful93] Fulton, William, *Introduction to Toric Varieties*, Annals of Mathematics Studies, no. 131, Princeton University Press, Princeton, New Jersey, 1993.
- [GV01] Gabrielov, Andrei and Vorobjov, Nicolai, “*Complexity of cylindrical decompositions of sub-Pfaffian sets*,” Effective methods in algebraic geometry (Bath, 2000), J. Pure Appl. Algebra 164 (2001), no. 1–2, pp. 179–197.
- [GKZ94] Gel’fand, Israel Moseyevitch; Kapranov, Misha M.; and Zelevinsky, Andrei V.; *Discriminants, Resultants and Multidimensional Determinants*, Birkhäuser, Boston, 1994.
- [Gri82] Grigor’ev, Dima Yu., “*Lower Bounds in the Algebraic Complexity of Computations*,” The Theory of the Complexity of Computations, I; Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov (LOMI) **118** (1982), pp. 25–82, 214.
- [GK96] Grigoriev, Dima and Karpinski, Marek, “*Computability of the Additive Complexity of Algebraic Circuits with Root Extracting*,” Theoretical Computer Science, vol. 157, no. 1, April 1996.
- [HS95] Huber, Birkett and Sturmfels, Bernd, “*A Polyhedral Method for Solving Sparse Polynomial Systems*,” Math. Comp. **64** (1995), no. 212, pp. 1541–1555.
- [Kal03] Kaloshin, V., “*The existential Hilbert 16-th problem and an estimate for cyclicity of elementary polycycles*,” Invent. Math. 151 (2003), no. 3, pp. 451–512.
- [Kat07] Katok, Svetlana, *p-adic Analysis Compared with Real*, Student Mathematical Library, vol. 37, American Mathematical Society, 2007.
- [Kho80] Khovanskii, Askold G., “*On a Class of Systems of Transcendental Equations*,” Dokl. Akad. Nauk SSSR **255** (1980), no. 4, pp. 804–807; English transl. in Soviet Math. Dokl. **22** (1980), no. 3.
- [Kho91] ———, *Fewnomials*, AMS Press, Providence, Rhode Island, 1991.
- [Koi96] Koiran, Pascal, “*Hilbert’s Nullstellensatz is in the Polynomial Hierarchy*,” DIMACS Technical Report 96-27, July 1996. (This preprint considerably improves the published version which appeared Journal of Complexity **12** (1996), no. 4, pp. 273–286.)
- [Koi10] Koiran, Pascal, “*Shallow Circuits with High-Powered Inputs*,” to appear in the proceedings of Innovations in Computer Science (ICS 2011, Jan. 6–9, 2011, Beijing China). Also available as Math ArXiv preprint [arXiv:1004.4960](https://arxiv.org/abs/1004.4960).

- [Len99] Lenstra (jr.), Hendrik W., “*On the Factorization of Lacunary Polynomials*,” Number Theory in Progress, Vol. 1 (Zakopane-Kóscielisko, 1997), pp. 277–291, de Gruyter, Berlin, 1999.
- [LRW03] Li, Tien-Yien; Rojas, J. Maurice; and Wang, Xiaoshen, “*Counting Real Connected Components of Trinomial Curves Intersections and m -nomial Hypersurfaces*,” Discrete and Computational Geometry, 30:379–414 (2003).
- [Mer96] Merel, Loic, “*Bounds for the torsion of elliptic curves over number fields*,” Invent. Math., 124(1–3):437–449, 1996.
- [Par99] Parent, Philippe, “*Effective Bounds for the torsion of elliptic curves over number fields*,” J. Reine Angew. Math, 508:65–116, 1999.
- [PRT09] Pébay, Philippe P.; Rojas, J. Maurice; and Thompson, David C., “*Optimization and $\mathbf{NP}_{\mathbb{R}}$ -Completeness of Certain Fewnomials*,” proceedings of SNC 2009 (August 3–5, 2009, Kyoto, Japan), pp. 133–142, ACM Press, 2009.
- [Poo98] Poonen, Bjorn, “*Zeros of sparse polynomials over local fields of characteristic p* ,” Math. Res. Lett. 5(3), pp. 273–279, 1998.
- [Ris85] Risler, Jean-Jacques, “*Additive Complexity and Zeros of Real Polynomials*,” SIAM J. Comput. 14 (1985), no. 1, pp. 178–183.
- [Roj02] Rojas, J. Maurice, “*Additive Complexity and the Roots of Polynomials Over Number Fields and p -adic Fields*,” Proceedings of ANTS-V (5th Annual Algorithmic Number Theory Symposium, University of Sydney, July 7–12, 2002), Lecture Notes in Computer Science #2369, Springer-Verlag (2002), pp. 506–515.
- [Roj03a] _____, “*Why Polyhedra Matter in Non-Linear Equation Solving*,” paper corresponding to an invited talk delivered at a conference on Algebraic Geometry and Geometric Modelling (Vilnius, Lithuania, July 29 – August 2, 2002), Contemporary Mathematics, vol. 334, pp. 293–320, AMS Press, 2003.
- [Roj03b] _____, “*Dedekind Zeta Functions and the Complexity of Hilbert’s Nullstellensatz*,” Math ArXiv preprint math.NT/0301111 .
- [Roj04] _____, “*Arithmetic Multivariate Descartes’ Rule*,” American Journal of Mathematics, vol. 126, no. 1, February 2004, pp. 1–30.
- [RSS10] Rusek, Korben; Sottile, Frank; and Shakalli-Tang, Jeanette, “*Dense Fewnomials*,” Math ArXiv preprint arXiv:1010.2962 .
- [Ser79] Serre, Jean-Pierre, *Local fields*, Graduate Texts in Mathematics, 67, Springer-Verlag, New York-Berlin, 1979.
- [Shu93] Shub, Mike, “*Some Remarks on Bézout’s Theorem and Complexity Theory*,” From Topology to Computation: Proceedings of the Smalefest (Berkeley, 1990), pp. 443–455, Springer-Verlag, 1993.
- [Sma98] Smale, Steve, “*Mathematical Problems for the Next Century*,” Math. Intelligencer 20 (1998), no. 2, pp. 7–15.
- [Sma00] _____, “*Mathematical Problems for the Next Century*,” Mathematics: Frontiers and Perspectives, pp. 271–294, Amer. Math. Soc., Providence, RI, 2000.
- [SL54] Smith, David Eugene and Latham, Marcia L., *The Geometry of René Descartes*, translated from the French and Latin (with a facsimile of Descartes’ 1637 French edition), Dover Publications Inc., New York (1954).
- [Stu94] Sturmfels, Bernd, “*Viro’s Theorem for Complete Intersections*,” Annali della Scuola Normale Superiore di Pisa, Classe di Scienze 4^e série, tome 21, n° 3 (1994), pp. 377–386.
- [VG03] Vakulenko, Sergey and Grigoriev, Dmitry, “*Complexity of gene circuits, Pfaffian functions and the morphogenesis problem*,” C. R. Math. Acad. Sci. Paris 337 (2003), no. 11, pp. 721–724.
- [Val79] Valiant, Leslie G., “*The complexity of computing the permanent*,” Theoret. Comp. Sci., 8:189–201, 1979.
- [Vir84] Viro, Oleg Ya., “*Gluing of plane real algebraic curves and constructions of curves of degrees 6 and 7*,” Topology (Leningrad, 1982), pp. 187–200, Lecture Notes in Math., 1060, Springer, Berlin, 1984.
- [Wan04] Wang, Xiaoshen, “*A Simple Proof of Descartes’ Rule of Signs*,” The American Mathematical Monthly, Vol. 111, No. 6 (Jun.–Jul., 2004), pp. 525–526, Mathematical Association of America, 2004.
- [Wil99] Wilkie, A. J., “*A theorem of the complement and some new o-minimal structures*,” Selecta Math. (N.S.) 5 (1999), no. 4, pp. 397–421.